CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Usporedba VPN poslužitelja

CCERT-PUBDOC-2008-11-246

+CERT.hr u suradnji s LSS

Sigurnosni problemi u računalnim programima i operacijskim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom CARNet CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Virtualna privatna mreža [VPN = Virtual Private Network] je tehnologija koja zadnjih godina privlači pažnju mnogih tvrtki i organizacija koje žele proširiti i/ili poboljšati postojeću infrastrukturu uz istovremeno smanjenje troškova poslovanja.

VPN se koristi onda, kad korisnik treba zaštićenu vezu između dvije (ili više) svojih adresa, ali ne može (zbog cijene ili nepostojanja tehničkih uvjeta) uspostaviti fizički ili virtualni prividni vod [PVC = Permanent Virtual Circuit].

VPN se uspostavlja kroz javnu telekomunikacijsku infrastrukturu (Internet), umjesto korištenja iznajmljenih veza. Zaštita i privatnost podataka se ostvaruje korištenjem tuneliranja i enkripcije prometa, kao i sigurnosnim procedurama koje jamče sigurnost podataka za vrijeme njihovog prijenosa putem Interneta.

Ovaj dokument daje opći pregled VPN tehnologije. Spomenuti su protokoli kojima se ona ostvaruje, metode primjene kao i najčešći sigurnosni rizici o kojima treba voditi računa prilikom primjene i korištenja ove vrste usluge. Dokument donosi pregled sigurnosnih rizika najpopularnijih VPN poslužitelja kao korisnike savjete kako smanjiti sigurnosne rizike u korištenju pristupa lokalnoj mreži s udaljenih lokacija.

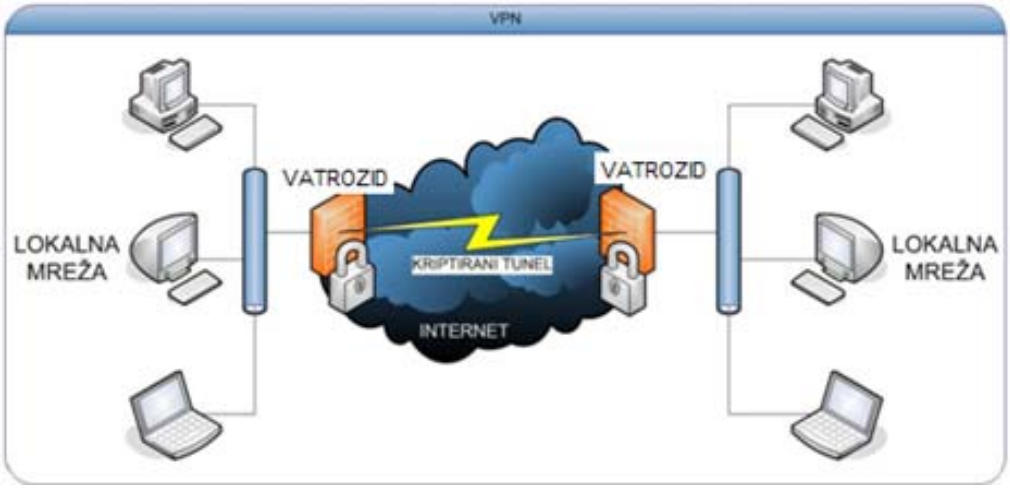
2. Opći pregled

VPN (eng. Virtual Private Network) predstavlja naprednu tehnologiju koja se koristi kod povezivanja udaljenih računala u tzv. virtualne privatne mreže, a pritom koristi dijeljenu ili javnu telekomunikacijsku infrastrukturu.

Riječ „virtualna“ označava da računala koja se spajaju na ovaj način ne moraju biti fizički, izravno povezana, već posredno, preko (javnih) mreža za prijenos podataka. Pojam „privatna“ znači da se očekuje da nitko neovlašten na može prisluškivati komunikaciju ili u njoj sudjelovati, tj. barem da ne može razumjeti komunikaciju, čak i ako presretne promet. To se osigurava tako da su podaci koji se izmjenjuju kriptirani te ih može pregledavati samo definirana skupina korisnika, koja ima odgovarajuće lozinke. „Mreža“ znači da su korisnici koji koriste VPN međusobno povezani na način da mogu izmjenjivati datoteke, informacije, komunicirati video konferencijom te dijeliti različite mrežne servise.

Njezinim se korištenjem, dakle, omogućuje povezivanje zemljopisno udaljenih poslovnica i/ili korisnika štiteći pritom privatnost njihovih podataka. Važno je da se VPN tehnologija može koristiti i s privremenih adresa tijekom putovanja i privremenog, jednokratnog korištenja tuđih komunikacijskih infrastruktura koje su u pravilu nesigurne, a mogu biti i neprijateljski nastrojene.

Slika 1. prikazuje osnovnu ideju koja stoji iza VPN tehnologije kojom se omogućuje sigurna razmjena podataka između korisnika.



Slika 1. Virtualna privatna mreža

2.1. Preduvjeti i mogućnost primjene VPN usluga

Za uspostavu VPN veze između udaljenih adresa potrebno je osigurati sljedeće minimalne zahtjeve:

1. Omogućen pristup Internetu na udaljenoj adresi. VPN pristup je moguće koristiti preko standardnih modemskih ulaza, ADSL pristupa, GPRS/EDGE/UMTS-a tehnologija, Wi-Fi tehnologije, itd.
2. Detaljno razrađen način primjene VPN povezivanja
3. Mrežna infrastruktura s jasno određenim IP adresnim planom

VPN rješenja se primjenjuju ovisno o postojećoj infrastrukturi kao i o trenutnim i budućim potrebama za uspostavom ovog tipa povezivanja. Obzirom na to, povezivanje može biti izvedeno:

1. Programski: ostvaruje se instaliranjem klijentske VPN aplikacije na strani onih koji se žele spojiti na udaljenu mrežu. Nudi veliku fleksibilnost kod upravljanja prometom, a preporučuje se koristiti ovaj način povezivanja kod ekstranet mreža ili kada se pojedinačni korisnici žele spojiti na središnju lokaciju (bilo da je riječ o radu od kuće ili radu s privremene adrese za vrijeme putovanja ili rada na terenu). Ovaj se tip povezivanja koristi iz razloga što takvi korisnici najčešće koriste opremu (usmjerivače i vatrozid) koja se razlikuje od one koja se koristi u privatnoj udaljenoj mreži (prema vrsti proizvođača opreme).
2. Korištenjem sklopovlja (eng. hardware): u tom se slučaju instalira oprema koja osigurava VPN povezivanje. Ovaj način spajanja osigurava veće brzine prijenosa podataka, ali je znatno skuplji o odnosu na programsku izvedbu. Osim toga, korištenjem ove mogućnosti, mijenja se i postojeća infrastruktura mreže. To se koristi kad se trajno povezuju dvije (ili više) udaljenih lokalnih mreža, a svaka imaju više korisnika i računala koja moraju moći komunicirati s „drugom stranom".
3. Kombinacijom sklopovlja i potrebne programske podrške

2.2. Način primjene i korištenja VPN tehnologije

S obzirom na način korištenja razlikuju se tri osnovne primjene VPN tehnologija:

1. Intranet

Ovaj se tip spajanja najčešće koristi za spajanje lokalnih mreža udaljenih podružnica tvrtke sa središnjom lokacijom u jedinstvenu privatnu mrežu upotrebom Internet infrastrukture (tzv. LAN-to-LAN povezivanje). Povezivanje se ostvaruje uspostavom veze VPN poslužitelja na obje strane (obje lokalne mreže).

Međutim, mogu se pojaviti sljedeći problemi:

- Nepostojanje standardiziranog mehanizma za enkripciju (neodgovarajuća zaštita podataka)
- Nekompatibilnost opreme različitih proizvođača koja se nalazi na pojedinim adresama (mogu se pojaviti problemi oko uspostave veze)
- Nemogućnost osiguravanja *end-to-end QoS* usluge (zahtijevana brzina, dostupnost, kašnjenje, prioritet podataka, itd.)

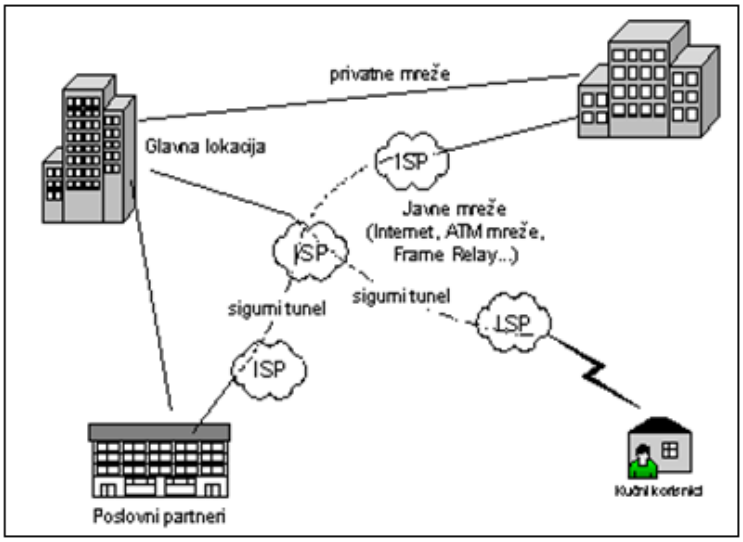
2. Ekstranet

Koristi se za povezivanje različitih poslovnih korisnika (npr. više različitih tvrtki) kako bi mogli izmjenjivati zajedničke resurse i podatke na siguran način. Ovom se metodom osigurava kontrolirani pristup pojedinim servisima dostupnim na privatnoj mreži. Pristup se ostvaruje spajanjem udaljenog VPN klijenta na VPN poslužitelj koji se nalazi na središnjoj adresi.

3. Rješenja za udaljeni pristup

Ovaj tip VPN rješenja koriste pojedinačni korisnici koji imaju potrebe za spajanjem na privatnu mrežu s udaljenih adresa. Ti se vanjski korisnici (koji primjerice rade od kuće ili su na terenu) spajaju na mrežu korištenjem klijentskog VPN programa za udaljeni pristup.

Slika 2. prikazuje spomenute načine povezivanja korištenjem različitih primjena VPN tehnologija.



Slika 2. Mogućnosti upotrebe VPN tehnologije (intranet, ekstranet, udaljeni pristup)

2.2.1. VPN kao zamjena za WAN - prednosti i nedostaci

Uslijed sve veće popularnosti i dostupnosti Interneta te usavršavanja i pojeftinjenja mrežne opreme koja se pritom koristi, VPN se posljednjih godina sve više koristi kao alternativno rješenje umjesto korištenja WAN mreža. WAN (eng. Wide Area Network) ili mreža širokog područja je ona koja se sastoji od više lokalnih mreža koje su međusobno povezane fizičkim, poprečnim, iznajmljenim vodovima ili privatnim prividnim vodovima (eng. Private Virtual Circuit)

VPN ne pruža nove funkcionalnosti koje se ne bi mogle ostvariti na neki drugi način (npr. preko WAN mreže), ali se u usporedbi s ostalim metodama VPN ističe kao, zasigurno, najjeftinija metoda.

Sljedeća tablica ukratko opisuje glavne razlike WAN i VPN mreža:

Opis usluge	WAN	VPN
Zajamčena brzina osiguravanja usluge na udaljenoj adresi	Da	Da/Ne
Omogućavanje usluge pristupa privatnoj mreži ograničenoj skupini ljudi	Da	Da
Sigurna komunikacija	Da/Ne	Da
Korištenje javno dostupne infrastrukture	Ne	Da

Tablica 1. Osnovne razlike WAN i VPN tehnologije

Do sad je u poslovnom svijetu WAN imao veliku prednost u odnosu na javne mreže po pitanju pouzdanosti, brzine i sigurnosti. Međutim, u usporedbi sa VPN-om, održavanje WAN mreža, koje koriste iznajmljene linije, može biti izuzetno skupo, posebice ako se radi o adresama koje su međusobno jako udaljene. Prednosti VPN-a očituju se u sljedećem:

- Fleksibilnost i skalabilnost mreže (moguće je u kratkom roku povezati nove ili privremene adrese što nije moguće kada se koriste iznajmljene linije)
- Umjesto zakupa iznajmljenih linija (ili spajanja korištenjem modema), kod VPN-a se plaćaju (samo) znatno niži troškovi za spajanje preko Interneta
- Manji trošak za nabavu i održavanje opreme koja se koristi

Bez obzira na popularnost, VPN nije savršeno rješenje i, kao i sve ostale tehnologije, ima svoja ograničenja. To su:

- Pouzdanost (dostupnost i brzina) – VPN ovisi o kvaliteti usluge ISP-a (pružatelja Internet usluga) koja nije uvijek zadovoljavajuća. Isto tako, ovisi i o načinu primjene VPN veze (koji protokoli se koriste, autentikacija, enkripcija, itd.).
- Nekompatibilnost opreme različitih proizvođača – što ima utjecaja prilikom primjene pojedinih standarda i protokola koji u tom slučaju neće raditi kako je predviđeno.
- Zahtijeva se vrhunsko poznavanje opreme koja se koristi u cilju ostvarivanja potpune zaštite privatne mreže od mogućih sigurnosnih prijetnji i napada. To uključuje poznavanje mrežnih protokola, sigurnosnih mehanizama i pažljivo konfiguriranje postavki sustava. Ljudi koji uspostavljaju, ali i održavaju VPN moraju biti visoko stručno osposobljeni i motivirani.

2.3. Osnovni koncept rada VPN tehnologije

U nastavku teksta slijedi objašnjenje principa rada VPN komunikacije koji koristi tehniku tzv. tuneliranja, te zaštitu podataka tijekom prijenosa javnim mrežama.

2.3.1. Tuneliranje

VPN mreža, preko javne mreže, stvara siguran kanal (tunel) između krajnjih točaka i tako stvara prividnu (eng. virtual) vezu između udaljenih adresa.

Tuneliranje, dakle, omogućuje prijenos podataka, namijenjenih korištenju samo unutar privatne mreže tvrtke, preko javne mreže na način da usmjerivači u javnoj mreži nisu „svjesni“ da je takav prijenos dio privatne mreže. Protokoli koji se koriste kod tuneliranja enkapsuliraju podatke (tj. pakete). Enkapsuliranje radi ovako:

- izvornom IP paketu (datagram) doda se posebno zaglavlje
- cijeli takav novi paket se stavlja u podatkovni prostor novog, „običnog“ IP datagrama koji se šalje izravno na adresu VPN poslužitelja s druge strane, na udaljenoj adresi
- s druge strane, primljeni se paket „otpakira“, analizira se posebno zaglavlje i zatim se izvorni IP paket šalje na odredište unutar te adrese putem interne, zaštićene mreže

Na taj način se postiže isti učinak kao da su dvije mreže spojene zasebnim linkom.

Osnovna prednost VPN tunela je što se njegovom upotrebom, po cijeni pristupa javnoj mreži, omogućuje sigurna razmjena podataka s korisničkih računala na udaljenim adresama kao da se ona nalaze na istoj adresi i spojena su u zaštićenu, lokalnu mrežu.

2.3.2. Sigurnosna zaštita kod VPN-a

Osim tuneliranja, a u svrhu zaštite, koriste se dodatni sigurnosni mehanizmi od kojih izdvajamo najbitnije:

1. **Autentikacija** – za osiguravanje ograničene provjere pristupa.
   Sam postupak autentikacije odnosi se na dokazivanje identiteta između korisnika koji se nalaze na krajevima tunela. VPN se sastoji od dva dijela: unutarnje mreže koja pruža fizičku i administrativnu sigurnost, i nezaštićene, vanjske mreže - Interneta. Obično se, između klijenta i poslužitelja, nalazi vatrozid. Kada klijent želi uspostaviti komunikaciju, podaci potrebni za autentikaciju se prosljeđuju autentikacijskom poslužitelju u zaštićenoj mreži. Ukoliko je klijent osoba od povjerenja, ovim postupkom može dobiti privilegije pristupa resursima koji nisu dostupni ostalim korisnicima. Tako se umanjuje rizik da napadač dobije pristup privatnoj mreži napadom na npr. računalo klijenta. Ovaj je podatak bitan sa stajališta sigurnosti jer dozvoljava da klijentsko računalo bude spojeno na javnu mrežu koja nije sigurna.

2. **Enkripcija** – za očuvanje povjerljivosti i integriteta podataka (nemogućnost izmjene postojećih sadržaja). Ovaj pojam označava postupak kodiranja podataka na način da ih u konačnici mogu pročitati (dekodirati) samo oni korisnici koji imaju potrebnu lozinku, dakle oni kojima su podaci i namijenjeni.

2.4. Način uspostave veze

Kao što je već rečeno, VPN pruža podršku za udaljeni pristup korisnika u privatnu mrežu preko Interneta, a temelji se na klijent/poslužitelj arhitekturi.

Uspostava veze odvija se ovim redoslijedom:

1. Udaljeni se korisnik spaja na Internet preko svog pružatelja Internet usluga (eng. ISP - Internet Service Provider),
2. Korisnik pokreće zahtjev za spajanjem na VPN poslužitelj tvrtke, VPN poslužitelj provjerava korisničko ime i lozinku, te dozvoljava daljnji rad
3. Kada se veza uspostavi udaljeni korisnik može komunicirati (npr. preuzimati podatke) s lokalnom mrežom kao da je svojim računalom izravno spojen na nju.

3. Protokoli tuneliranja

Korisnici VPN usluga mogu koristiti različite programske pakete koji im omogućuju jednostavno rukovanje VPN vezama. Ti paketi podržavaju stvaranje sigurnih tunela, postavljanje potrebnih konfiguracijskih parametara i spajanje na VPN poslužitelje. Uspješna komunikacija je moguća samo ako se koriste jednaki protokoli na obje strane, a najpoznatiji od njih su IPSec, SSL, PPTP i L2TP, čiji opisi slijede u nastavku teksta.

3.1. IPsec protokol

IPsec (eng. Internet Protocol Security) je standard i skup protokola (opcionalan za IPv4, a obavezan za IPv6) koji obuhvaćaju mehanizme za zaštitu prometa na razini trećeg sloja OSI mrežnog modela.

OSI model je apstraktni opis dizajna protokola komunikacijskih i računalnih mreža. Podijeljen je u sedam slojeva (fizički, podatkovni, mrežni, transportni, sloj sesije, prezentacijski i aplikacijski), gdje svaki sloj opisuje skup povezanih funkcija koje omogućuju jedan dio računalne komunikacije. Svih sedam slojeva zajedno, prikazuju tok podataka od izvora prema odredištu. Mrežni sloj pruža usluge povezanosti i odabira najbolje putanje za paket podataka.

IPsec arhitektura je opisana u dokumentu RFC 2401.

Korištenjem ovog protokola za VPN veze osiguravaju se sljedeći sigurnosni zahtjevi:

- tajnost i integritet podataka
- autentičnost
- raspoloživost (podaci su dostupni i kod neočekivanih događaja kao što je primjerice DoS napad)

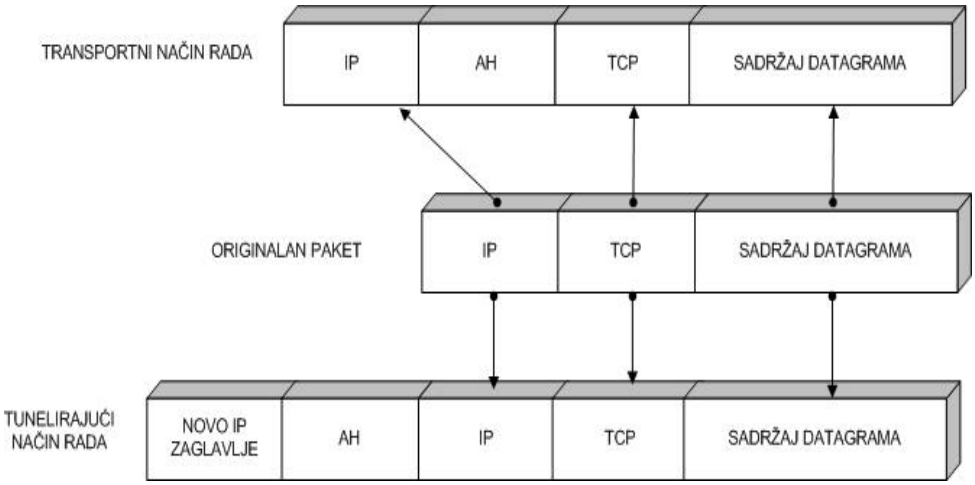
Kako bi osigurao autentikaciju, integritet i pouzdanost komunikacije IPsec koristi tri različita protokola, AH, ESP i IKEv2:

- **AH** (eng. Authentication Header) protokol za osiguranje nepovredivosti podataka i njihove autorizacije.
- **ESP** (eng. Encapsulated Security Payload) protokol omogućuje enkripciju i nepovredivost podataka
- **IKEv2** protokol se koristi se za stvaranje i distribuiranje kriptografskih ključeva. IKEv2 je poboljšana inačica protokola IKEv1 po pitanju sigurnosti (manji je rizik od DoS napada) i jednostavnosti (odnosi se na pojednostavljenje samog protokola čime se olakšava njegova primjena)

Naime, moguće je zaštititi cijeli IP datagram, ili pak samo protokole višeg sloja. Stoga postoje dva primarna načina rada:

1. **Tunelirajući** – IP datagram je u potpunosti enkapsuliran novim datagramom koristeći IPsec protokol. Koristi se za komunikaciju računala u lokalnoj mreži.

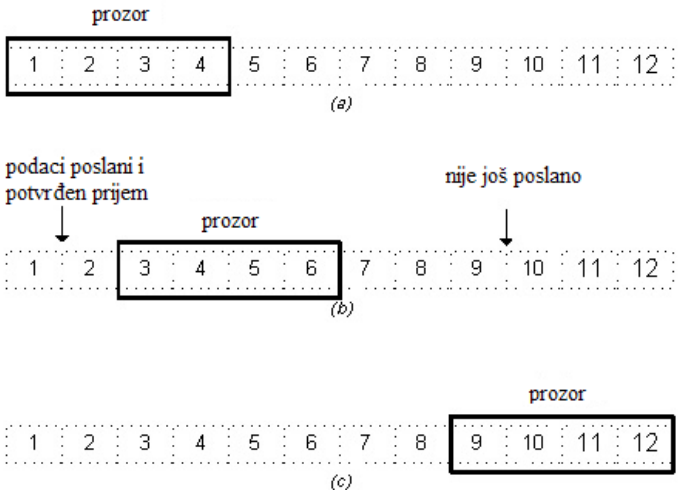
2. **Transportni** – obavlja se zaštita podataka viših protokolnih slojeva, a IPsec zaglavlje se umeće između originalnog IP zaglavlja i zaglavlja protokola bez kriptiranja. Ova se metoda koristi za razmjenu podataka u VPN vezama.



Slika 3. Dodavanje zaglavlja kod IPsec protokola
Izvor: AngelFire

Za zaštitu integriteta podataka primjenjuju se SHA i MD5 algoritmi (kao i kod SSL protokola). Da bi se zaštitio sadržaj paketa koriste se simetrični algoritmi kriptiranja. IPsec standard zahtijeva minimalno implementaciju NULL i DES algoritama, no danas se koriste i češći su jači algoritmi kao što su 3DES i AES.

Pomoću mehanizma tzv. „klizećih prozora" (eng. sliding window) IPsec pruža zaštitu od DoS (eng. Denial of Service) napada. To znači da se svakom paketu pridružuje određeni redni broj i paket se dostavlja samo u slučaju da se njegov redni broj nalazi u promatranom prozoru ili je noviji. Svi stariji paketi se automatski odbacuju. Ovaj postupak štiti od napada snimanjem i ponavljanjem (eng. replay attack), u kojima napadač snimljene originalne pakete pokušava ponovno poslati (npr. ako napadač snimi enkriptiranu novčanu transakciju te istovjetne pakete ponovno „ubaci" u komunikacijski kanal). Slika 4 prikazuje i objašnjava spomenuti sigurnosni mehanizam za prijenos četiri okteta podataka. Krećući se s lijeva na desno, prozor „klizi" kako se pojedini bajt pošalje i potvrdi njegov prijem.



Slika 4 . Mehanizam klizećih prozora

Osim toga, IPsec koristi dvije vrlo bitne baze podataka čiji se zapisi nalaze u samoj jezgri operacijskog sustava:

a) **Baza podataka sigurnosne politike** (eng. SPD - Security Policy Database). U SPD bazi administrator definira sigurnosnu politiku (eng. security policy) i to na način da odredi raspon IP adresa za zaštićeni promet, koji protokol se koristi, razina zaštite, itd.
b) **Baza podataka sigurnosnih asocijacija** (eng. SAD - Security Association Database). SAD baza podataka čuva tzv. sigurnosne asocijacije, koje su zapravo skup sigurnosnih parametara, npr. kriptoalgoritmi korišteni u komunikaciji. Svako sigurnosno udruživanje jedinstveno je definirano protokolom (AH ili ESP), odredišnom IP adresom i indeksom sigurnosnog parametra (eng. SPI - Security Parameters Index). Zapisi u jednoj i drugoj bazi nalaze se u samoj jezgri operacijskog sustava.

Obzirom na opisane funkcionalnosti i mehanizme zaštite IPsec predstavlja najsigurniji protokol u VPN komunikaciji te ga se kao takvog najčešće koristi za sigurnu razmjenu podataka preko javne mreže.

3.2. PPTP protokol

PPTP (eng. Point to Point Tunneling Protocol) je mrežni protokol koji osigurava siguran prijenos podataka s udaljenog klijenta na privatnu mrežu preko Interneta ili neke druge mreže koja se temelji na TCP/IP protokolu.

Razvio ga je konzorcij proizvođača tvrtki US Robotics, Ascend Communications, 3Com, ECI Telematics i Microsoft. Izvorno je PPTP zamišljen kao mehanizam za enkapsulaciju paketa podataka koji bi omogućavao prijenos protokola koji nisu temeljeni na TCP/IP stogu (npr. IPX i AppleTalk preko Interneta) korištenjem GRE (eng. Generic Routing Encapsulation) enkapsulacije. Za stvaranje i održavanje tunela koristi se TCP protokol (TCP priključak 1723), dok se za tuneliranje PPP paketa koristi GRE enkapsulacija (IP protokol 47).

GRE je protokol ovijanja koji osigurava mehanizam za enkapsulaciju paketa unutar transportnog protokola. Sadržaj se najprije enkapsulira u GRE paket, koji u sebi može sadržavati podatke o ruti. Dobiveni GRE paket tada se enkapsulira u neki drugi protokol i prosljeđuje (protokol isporuke). GRE se uglavnom koristi s IP protokolom na način da koristi ovaj protokol za isporuku ili za sadržaj.

PPTP je proširenje mrežnog protokola PPP (eng. Point-to-Point Protocol) čime se omogućuje uspostava VPN veze. PPTP osigurava autentikaciju i kompresiju, ali mu je sigurnost slabija strana. Metode koje se koriste za autentikaciju sadrže sigurnosne propuste koje napadači vrlo često koriste za otkrivanje pristupnih lozinki i tako pristup privatnoj mreži. Autentikacija se ostvaruje korištenjem protokola MS-CHAP, MS-CHAPv2, a enkripcija preko RC-4 ILI MPPE algoritma.

Kako radi?

Kada PPTP poslužitelj (tj. računalo koje je istovremeno spojeno na javnu i privatnu mrežu) primi paket s javne mreže, on ga dalje šalje privatnom mrežom do odredišnog računala. To obavlja obradom enkapsuliranog paketa u kojem je definirana adresa odredišta.

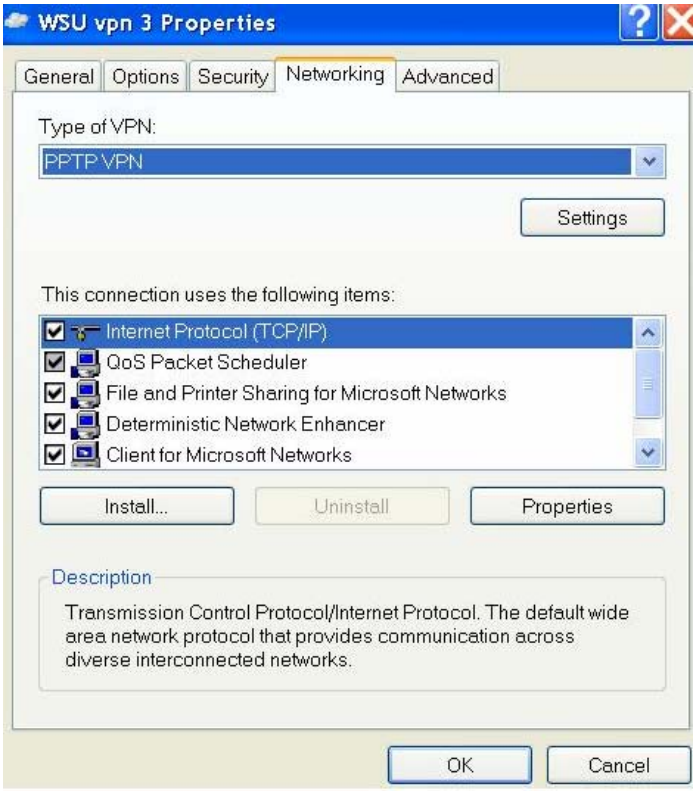
Moguća su dva oblika povezivanja na PPTP poslužitelj preko Interneta:

3.2.1. Kada ISP nema instaliranu podršku za PPTP

Klijent se najprije mora PPP vezom spojiti na ISP (kako bi imao vezu na Internet). Zatim se mora stvoriti druga logička veza kojom se klijent povezuje sa VPN poslužiteljem. Klijent u tom slučaju mora imati instaliran PPTP upravljački program kako bi mogao ostvariti zasebne veze na ISP i PPTP poslužitelj.

Instaliranje PPTP klijenta:

- Start → Settings→ Control Panel → Network connections → Create new connection
- Zatim redom odabrati mogućnosti: Connect to the Network at my Workplace, Virtual Private Network i definirati potom željenu adresu za spajanje. Završiti stvaranje veze u skladu s ponuđenim mogućnostima.
- Nakon toga na ikoni nove veze unijeti osobne podatke potrebne za spajanje (korisničko ime i pristupna lozinka), odabrati na Properties → Security i definirati da se za VPN koristi PPTP protokol.

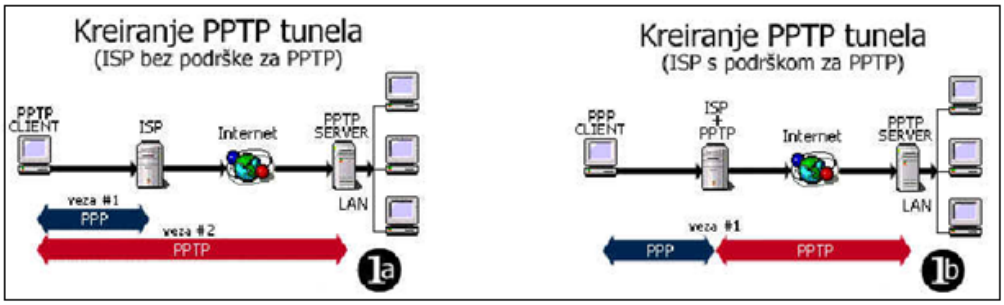


Slika 5.Uspostava PPTP VPN veze

- Nakon toga moguće je spajanje na udaljeni poslužitelj

3.2.2. ISP ima instaliranu podršku za PPTP

Ako je na ISP-u instalirana podrška za PPTP, tada nije potrebno instalirati nikakav dodatni program kod korisnika za PPTP komunikaciju. U tom slučaju ISP omogućuje PPP vezu, a podatke prosljeđuje uspostavljajući PPTP vezu sa odredišnim PPTP poslužiteljem.



Slika 6. Uspostava veze pomoću PPTP protokola

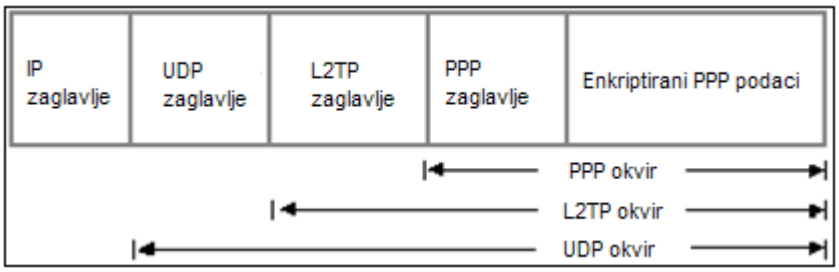
Izvor: AngelFire

3.3. L2TP i L2TP/IPsec

L2TP (eng. Layer 2 Tunneling Protocol) je IETF standard koji je nastao kombinacijom funkcionalnosti PPTP i L2F (eng. Layer 2 Forwarding Protocol) protokola, karakterističnog za Cisco uređaje.

L2TP radi na drugom sloju OSI modela i koristi se kao protokol tuneliranja za IP, X.25, Frame Relay ili ATM mreže.

Princip rada je takav da se osnovnom paketu (koji se šalje mrežom) dodaje L2TP zaglavlje na što se dodaje UDP zaglavlje (koristi se izvorišni i odredišni priključak 1701). Na kraju, paket se enkapsulira dodavanjem IP zaglavlja koje sadrži IP adrese klijenta i poslužitelja.



Slika 7. Način prijenosa podataka korištenjem L2TP protokola

Izvor: Best Computer EBooks

Krajnje točke L2TP tunela se nazivaju LAC (eng. L2TP Access Concentrator) i LNS (eng. L2TP Network Server). LAC se nalazi na strani klijenta koji želi uspostaviti VPN vezu, a LNS predstavlja poslužiteljsku stranu koja zaprima zahtjeve za uspostavom tunela.

Budući da je L2TP protokol koji koristi slabu autentikaciju (EAP, CHAP, SPAP) i ne omogućuje enkripciju, uglavnom se koristi u kombinaciji s IPsec protokolom. Ova je kombinacija poznata kao **L2TP/IPsec** standard koji je definiran dokumentom RFC 3193.

Uspostava veze odvija se na sljedeći način:

1. Pregovaranje o IPsec Security Association (SA), komunikaciji preko UDP priključka 500. Autentikacija se odvija korištenjem certifikata ili zajedničkog ključa. Pritom obje strane koriste zajedničku lozinku, javni ključ ili X.509 certifikat
2. Uspostava Encapsulating Security Payload (ESP) komunikacije čime se uspostavlja siguran kanal koji koristi IPsec enkripciju
3. Pregovaranje i uspostava L2TP veze (na UDP priključku 1701) između klijenta i poslužitelja
4. Razmjena informacija i podataka

U tom je slučaju sigurnost zajamčena korištenjem AH i ESP protokola. Svi podaci koji se nalaze u sklopu L2TP paketa se IPsec sustavu čine kao jedinstveni (homogeni) IP podatkovni paket te se na siguran način mogu prenositi preko javne mreže. Međutim, ovaj protokol može imati problema s određenim vatrozidima jer zahtijeva da su otvoreni priključci UDP 1701, IPsec IKE i UDP 500 što većina vatrozida na javnim mjestima ne dozvoljava (uglavnom su otvoreni HTTP i HTTPS priključci i TCP 80).

3.4. SSL protokol

SSL (eng. Secure Sockets Layer) je transportni protokol kojeg je razvila tvrtka Netscape Communications kako bi omogućila sigurnu i zaštićenu komunikaciju sugovornika preko javne mreže. Njegova je osnovna prednost što nije potrebno instalirati poseban program za spajanje na poslužitelj nego se komunikacija odvija preko web preglednika tako da je pogodan za povremene korisnike (udaljeni djelatnici, poslovni partneri, itd.).

Za uspostavu zaštićenog prijenosa podataka SSL zahtijeva minimalno identifikaciju poslužitelja. Nakon uspješne identifikacije klijent i poslužitelj mogu razmjenjivati kriptirane poruke štiteći tako podatke od prisluškivanja i neovlaštene izmjene.

Za svoj rad koristi dva protokola:

Protokol	Opis
SSL Handshake	Omogućuje klijentu i poslužitelju međusobnu identifikaciju. Identitet strana koje sudjeluju u komunikaciji osigurava se primjenom digitalnog potpisa i javnih ključeva. Koriste se algoritmi RSA i DSS. Kada SSL klijent i SSL poslužitelj prvi puta počnu komunicirati, dogovaraju se o inačici protokola, algoritmu za kompresiju i odabiru algoritama za simetrično kriptiranje nakon čega mogu započeti s razmjenom podataka. Još jedna prednost korištenja SSL algoritma leži u činjenici kako je veza pouzdana jer se provjerava integritet datoteka ili poruke prilikom prijenosa između pošiljaoca i primatelja. U tu se svrhu koriste algoritmi SHA i MD5.
SSL Record	Ovaj je protokol zadužen za kriptiranje i prijenos poruka. To radi tako da prima podatke od aplikacijskog sloja u blokovima proizvoljnih duljina. Same podatke ne interpretira, već ih fragmentira u blokove fiksne dužine (veličine 2^{14} bajtova ili manje), koje zaštiti i šalje sugovorniku, gdje se odvija obrnuti proces. Tako više klijentskih poruka može biti spojeno u jedan fragment ili jedna poruka podijeljena u više fragmenata. Ti se podaci potom komprimiraju i zaštićuju korištenjem algoritama za simetrično kriptiranje – DES i RC4. Na taj se način, u odnosu na asimetrične ključeve, postiže veća brzina rada - ta brzina možda nije toliko bitna kada se poslužuje jedan korisnički zahtjev, ali ako se radi o velikom broju zahtjeva koji se poslužuju paralelno, bolje je koristiti simetrični sustav .

Tablica 2. Mehanizmi zaštite kod SSL protokola

3.5. Usporedba VPN protokola

IPsec omogućuje bolje performanse sustava (brža je razmjena podataka) u odnosu na PPTP protokol, ali je tuneliranje prometa ograničeno samo na IP pakete. Nadalje, IPsec pruža jače mehanizme enkripcije od PPTP koji koristi RC4 algoritam (koji je slabiji u odnosu na npr. 3DES algoritam).

Više detalja o postojećim algoritmima za enkripciju moguće je pogledati na web stranici:

http://www.users.zetnet.co.uk/hopwood/crypto/scan/

Da bi se IPsec koristio, na svako računalo mora biti instaliran poseban klijentski program (s uključenim licencama), što nije slučaj s PPTP kojeg je zato jednostavnije primijeniti i koristiti.

Iako L2TP/IPsec omogućuje bolju zaštitu korištenjem IPsec funkcionalnosti, u usporedbi sa PPTP ima značajan nedostatak. Neke manje tvrtke/organizacije koriste samo jednu javnu adresu za pristup

Internetu, a lokalna računala koja su povezana na tu privatnu mrežu koriste privatne adrese. Tako nastaje problem kod L2TP tunela jer paket putuje javnom mrežom i u trenutku kada stigne na adresu na koju je poslan ne može se jamčiti njegova isporuka (jer može biti predviđen za bilo koje računalo koje je skriveno iza te javne mreže). U tom se slučaju takav paket odbacuje. Kod takvih se mreža zato preporučuje korištenje PPTP protokola.

SSL protokol se preporuča korisnicima koji se spajaju na aplikacije tvrtke koje se temelje na webu (eng. web-based applications), ali ako se želi osigurati pristup povjerljivim informacijama savjetuje se koristiti jaču enkripciju koju pruža IPsec. S druge strane, za implementaciju SSL veze nisu potrebna nikakva ulaganja niti dodatni klijentski programi što je mnogima od velike važnosti.

PPTP ponajviše koriste manje tvrtke i organizacije iz razloga što klijentski program dolazi u paketu s licenciranom inačicom operacijskih sustava Windows te kao takav ne zahtijeva nikakva dodatna ulaganja (a besplatna je inačica dostupna i za ostale platforme kao što su Linux, FreeBSD, i dr.). Korisnicima se pritom savjetuje korištenje dostupnih mehanizama za autentikaciju i enkripciju uz upotrebu složenih (i nasumičnih) zaporki.

Uobičajena primjena SSL protokola je u Internet preglednicima kad je potrebno osigurati povjerljivost podataka kod pristupa pojedinim web stranicama i/ili za pregled i razmjenu poruka elektroničke pošte.

L2TP primarno koriste pružatelji usluga kako bi saželi i prenijeli VPN promet kroz back-bone arhitekturu.

IPsec je IETF protokol razvijen prvenstveno radi zaštite VPN prometa koji vodi brigu o cjelovitosti podataka i sigurnosti. Koristi se ponajviše za VoIP komunikaciju (eng. Voice Over IP) i za pristup posebnim aplikacijama pojedine tvrtke ili organizacije.

Kao što se može vidjeti, svi spomenuti protokoli koji se koriste u VPN vezama imaju svoje prednosti i nedostatke po pitanju zaštite podataka i načina primjene. Stoga je na tvrtkama je da najprije detaljno prouče sve mogućnosti, odluče koji tip VPN veze bi najbolje zadovoljavao zahtjeve za uspješnim funkcioniranjem njihove organizacije te ih zatim primjenjuju.

4. Različite primjene VPN tehnologije

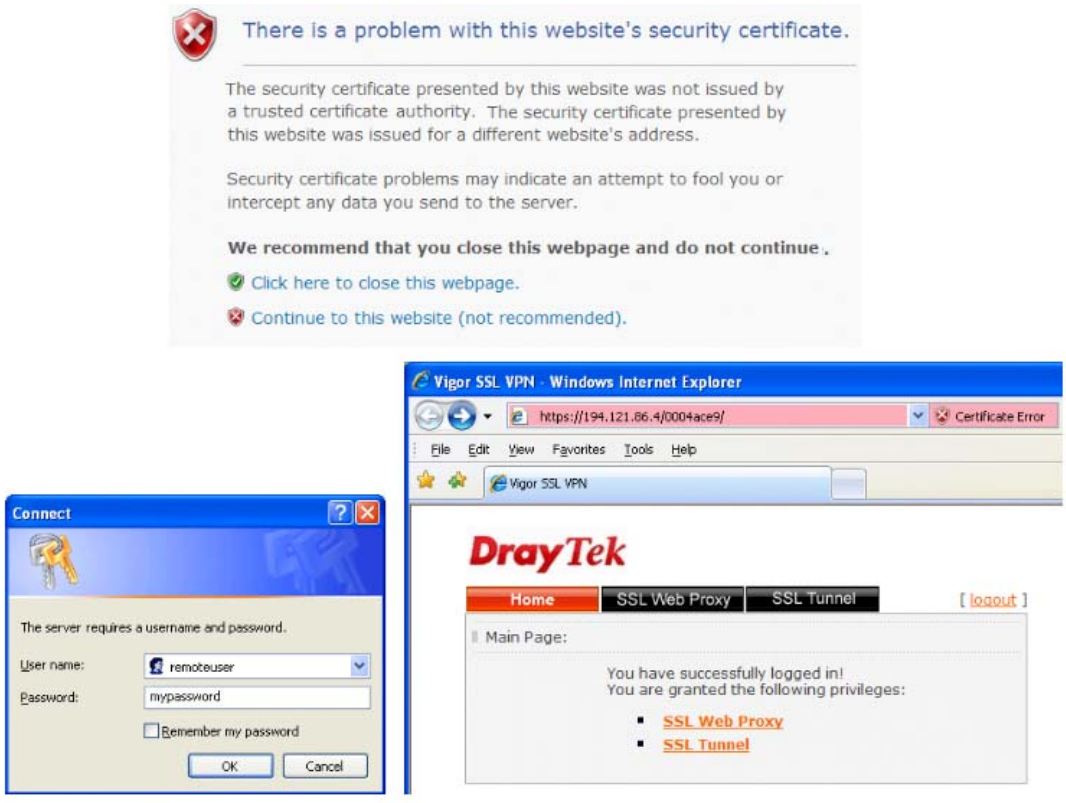
Trenutno na tržištu postoji niz VPN primjena od kojih su opisane najčešće korištene.

4.1. Open VPN

Ovaj način povezivanja korisnicima nudi iste mogućnosti povezivanja kao i puno poznatiji proizvodi, ali ključna je razlika u činjenici da se radi o programskom rješenju otvorenog koda.

Aplikacija je realizirana pod Open Source GNU GPL licencom (što znači da ju se može besplatno preuzeti preko Interneta i instalirati) i moguće ju je instalirati na gotovo svim danas popularnim platformama (MS Windows, Linux, Mac OS X, OpenBSD, FreeBSD i NetBSD).

Za uspostavu komunikacije koristi SSL protokol. Tako se ostvaruje slična sigurnost kao i u mrežama koje koriste IPsec protokol. Kod većine VPN rješenja temeljenih na SSL protokolu nije potrebno posebno konfigurirati klijenta jer se veza uspostavlja putem web preglednika (u adresno se polje upisuje adresa na koju se korisnik želi spojiti, potvrđuje se da se želi pristupiti stranici i nakon unosa korisničkih podataka uspostavlja se VPN veza – slika 8).



Slika 8. Uspostava VPN preko web preglednika

Međutim u ovom je slučaju situacija malo drugačija: ista se aplikacija mora instalirati na poslužitelju i na klijentu. Osnovno podešavanje je vrlo jednostavno, ali kompleksnost primjene raste ovisno o složenosti topologije mreže. OpenVPN je moguće koristiti za stalno i/ili povremeno povezivanje pojedinih adresa i uređaja. Za više detalja savjetuje se pogledati upute na stranici:

http://openvpn.net/index.php/documentation/install.html

Svi podaci koji se šalju preko mreže se kriptiraju i usmjeravaju na TCP ili UDP priključak (uobičajeno je korištenje UDP priključka 1194). Pitanje autentikacije (i time onemogućavanje aktivnih napada) se rješava korištenjem HMAC (eng. keyed-hash message authentication code) funkcije, a upotrebljava se uz kriptografske funkcije (MD5 ili SHA) i sigurnosni ključ.

Kako bi se spriječili napadi snimanjem i ponavljanjem, OpenVPN koristi mehanizam „klizećih prozora" korištenjem SWA algoritma (eng. Sliding Window Algorithm).

Glavna prednost Open VPN-a je njegova jednostavnost u primjeni. Koristi napredne kriptografske algoritme, ali ne opterećuje pretjerano resurse računala na kojem je instaliran. Uz sve to je i besplatan, pa se za manje korisnike može smatrati povoljnim rješenjem za ostvarivanje VPN veza.

4.2. Microsoft VPN rješenje

Za uspostavu VPN veze kod instaliranih operacijskih sustava Windows moguće je koristiti programske pakete tvrtke Microsoft koja se sastoji od klijentske i poslužiteljske strane. Microsoft VPN veza može se temeljiti na PPTP ili L2TP/IPsec protokolima. Sličnosti korištenja su:

- Osiguravaju razmjenu PPP okvira
- Omogućuju tuneliranje, enkapsulaciju paketa i mehanizme za autentikaciju korištenjem korisničkog imena i pristupne lozinke

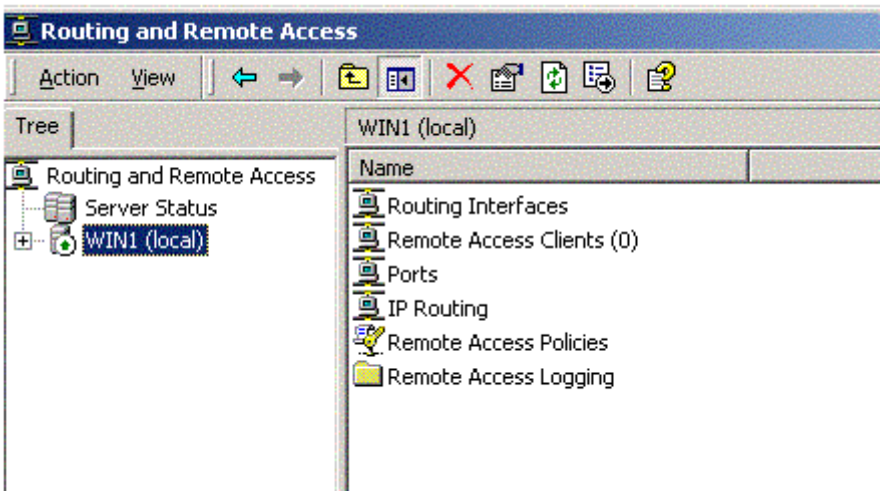
Prednosti L2TP/IPsec nad PPTP su:

1. Kod PPTP enkripcija se radi nakon PPP autentikacije. IPsec osigurava autentikaciju paketa, integritet i povjerljivost podataka korištenjem enkripcije prije PPP autentikacije tako da su i korisnički podaci također sigurni
2. PPTP koristi RC-4 enkripciju, a L2TP/IPsec koristi DES algoritam
3. Jaki mehanizmi autentikacije: na razini IPsec sesije provodi se autentikacija računala pomoću certifikata i javnog ključa, a zatim korisnička autentikacija (korisničko ime i pristupna lozinka) za enkriptirane L2TP paketa. Time se onemogućuju tzv. „dictionary" napadi kojima je moguće saznati tajne podatke o korisnicima. Kod PPTP postoji samo autentikacija na razini korisnika.
4. Moguće je uspostaviti vezu s uređajima koji nisu na javnoj mreži nego su se nalaze iza NAT prevoditelja mrežnih adresa.

U nastavku je opisan način instaliranja P2TP/IPsec VPN veze na platformi Win XP.

Instalacija na strani Windows poslužitelja:

1. Start → Control Panel → Administrative Tools → Routing and Remote Access. Radi se o standardnom servisu u sklopu Win2k3 sustava. U ovom se meniju postavljaju parametri kako bi vanjski korisnici imali pristup poslužitelju te kako bi se primijenile određene sigurnosne politike (eng. Remote Access Policies)

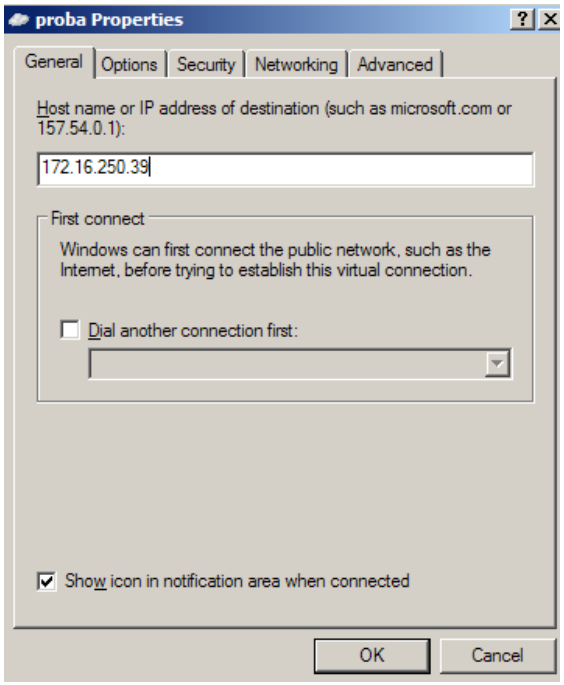


Slika 9. Okvir „Routing and Remote Access“

2. U okviru Common Configurations izabere se Virtual private network (VPN server) → Remote Client Protocols (gdje se uključuje podrška za TCP/IP)
3. U okviru Internet Connection izabire se način spajanja na Internet
4. U okviru Add Certificate Services definira se korištenje certifikata, princip razmjene ključeva, protokoli za autentikaciju (MS-CHAPv2-Microsoft Challenge Handshake Authentication Protocol version 2 ili EAP - Extensible Authentication Protocol)
5. U okviru IP Address Assignment se definiraju adrese računala koja će se spajati na poslužitelj
6. Klikne se na Ports → Properties → WAN Miniport → Configure kako se bi postavio maksimalan broj istovremenih VPN veza te hoće li se mrežna kartica koristiti samo za dolazni promet ili je moguće i slanje podataka s poslužitelja
7. Potom se definiraju Dial-in karakteristike: Start → Control Panel → Network Connections → Create new connection → Set up advanced connection → Accept incoming connections → Allow virtual private connection
8. Definiraju se korisnici koji imaju pravo pristupa
9. Ukoliko je poslužitelj spojen na mrežu preko usmjerivača potrebno je još samo u okviru „Port Mapping“ na usmjerivaču postaviti uobičajeni priključak za prihvat prometa (za PPTP je to 1723)

Instalacija na strani klijenta koji ima instaliran Windows XP:

1. Start → Control Panel → Network Connections → Create new connection → Connect to the network at my workplace → Virtual Private Network connection gdje se upisuje naziv veze i IP adresa poslužitelja
2. Odabrati na ikonu nove veze
3. Upisati korisničke podatke te odabrati na mogućnost Properties. Otvara se novi prozor:



Slika 10. Postavljanje parametara VPN veze za Microsoft platforme

4. Postaviti podatke u okvirima Security te Networking (definirati koji se protokol koristi, da li se koristi enkripcija itd.)
5. Nakon toga moguće je koristiti VPN klijent te se spojiti na udaljeno računalo

4.3. Cisco Easy VPN

I tvrtka Cisco ima rješenje kako ostvariti sigurnu i pouzdanu VPN vezu. Riječ je o programu Cisco Easy VPN koji centralizira rad Cisco uređaja. Time se rješava problem kompleksnog upravljanja i konfiguriranja VPN mreže, tako da korisnici koji se spajaju imaju što manje posla prilikom uspostave veze.

Dvije osnovne komponente sustava su opisane u tablici 3:

Komponenta	Opis
Easy VPN Remote funkcionalnost	Omogućuje udaljenim uređajima/VPN klijentima jednostavnu implementaciju sigurnosnih politika za VPN vezu preko poslužitelja. Dostupan je za uređaje Cisco 800,1700, 1800, 2800, 3800, UBR 900 seriju, ASA 5505, Cisco PIX 501 i 506E uređaje kao i za Cisco VPN klijentski program koji se instalira na strani korisnika
Easy VPN poslužitelj	Koristi se za centralizirano upravljanje svim parametrima komunikacije (primjena sigurnosne politike, enkripcija, autentikacija itd.) Pogodan je za Cisco 800,1700, 1800, 2800, 3800, 7200 seriju usmjerivača, 7301 seriju te za sve Cisco ASA i PIX uređaje.

Tablica 3. Osnovne komponente Cisco Easy VPN rješenja

Ovo je rješenje moguće prilagoditi za gotovo sve vrste poslovnih rješenja, a pogodni su za korištenje iz sljedećih razloga:

- Zaštita od virusa, crva, itd.
- Jedan uređaj za ostvarivanje SSL VPN i IPsec VPN veza
- Kompresija podataka
- Pregledno grafičko sučelje za prilagodbu rada
- Centralizirani mehanizam za stvaranje i primjenu sigurnosnih politika
- Integrirani vatrozid, idr.

Klijent može koristiti platforme:

- Windows 98, ME, NT4, 2000, ili Windows XP
- Linux
- Solaris Unix
- Mac OS X 10.2

Instaliranjem klijentskog programa uspostavlja se sigurna, kriptiranja veza na bilo koji Cisco Easy VPN poslužitelj. Princip rada je takav da kada korisnik inicira vezu za Cisco IOS VPN uređaj, najprije slijedi autentikacija uređaja korištenjem IKE mehanizma nakon čega slijedi autentikacija na razini korisnika korištenjem protokola RADIUS ili TACACS+ .

Karakteristike Cisco Easy VPN poslužitelja:

Opis	Što podržava
Protokoli tuneliranja	IPSec Encapsulating Security Payload (ESP), PPTP, L2TP, L2TP/IPSecn Network Address Translation (NAT) Transparent IPsec, Ratified IPsec/UDP, IPsec/TCP
Enkripcija/autentikacija	IPsec (ESP) korištenjem protokola Data Encryption Standard (DES)/Triple DES (3DES) (56/168-bita) ili AES (128/256-bita) sa MD5 ili SHA
Kompresija podataka	Lempel-Ziv standard (LZS)
Upravljanje ključevima	IKE mehanizam

Tablica 4. Cisco Easy VPN poslužitelj - karakteristike

Instalacija Cisco VPN klijenta obavlja se pomoću programskog paketa Cisco Systems VPN, dok se za poslužitelj koristi paket Cisco Router and Security Device Manager (SDM) pomoću kojeg se pojednostavljuje konfiguriranje VPN poslužitelja preko jednostavnog grafičkog sučelja. Implementiranje Cisco Easy VPN klijenta je besplatno dok cijena za poslužitelja ovisi o tipu uređaja na kojem se ova usluga primjenjuje, broju korisnika kao i o tome nabavlja li se potpuno novi uređaj ili se radi o nadogradnji postojećeg.

4.4. Hamachi

LogMeIn Hamachi je jedna od novijih VPN aplikacija za operacijske sustave Windows, Linux i OS X. Jednostavno ga je instalirati i koristiti, a ponajviše se koristi za umrežavanje i igranje preko Interneta. Cjelokupno se rješenje, kao i u prethodnim primjerima, zasniva na modelu klijent-poslužitelj.

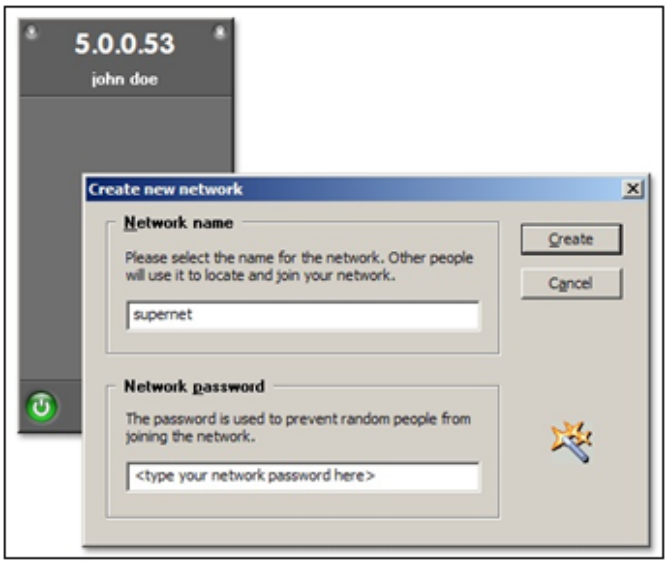
Prednosti:

- Omogućuje povezivanje više računala u sigurnu mrežu.
- Pristup kritičnim datotekama i mrežnim uređajima,
- Nije potrebno dodatno podešavati usmjerivač niti vatrozid,
- Provjera pristupa za korisnike, korištenje enkripcije i autentikacije,
- Veza je uspješno uspostavljena u 95% slučajeva
- Osnovna inačica programa je besplatna. Tzv. „Premium“ inačica iznosi $4,95 mjesečno (razlikuje se s obzirom na besplatnu inačicu prema broju korisnika, mogućnosti razmjene poruka, ovlastima za upravljanje mrežom itd.)

Nedostaci:

Kao bitan nedostatak ističe se činjenica da nije moguće sigurno pretraživati Internet s računala na udaljenoj adresi koje je istovremeno spojeno na privatnu mrežu.

Instalacija je jednostavna: nakon preuzimanja programskog paketa putem Interneta pokreće se instalacija. Po završetku instalacije potrebno je stvoriti mrežu (naziv i lozinka)



Slika 11. Stvaranje veze za Hamachi VPN

Svakom se novom korisniku dodijeli posebna adresa oblika 5.x.x.x. Nakon toga potrebno je definirati i adrese računala koje će se spajati na poslužitelj (upisuju se dodijeljene adrese). Ostali se korisnici zatim spajaju na tu istu mrežu. Svaki Hamachi korisnik ima ovlasti nad instaliranim programom kako bi mogao upravljati pristupnom lozinkom, „zaključavati“ mrežu, dodjeljivati/zabraniti pristupne ovlasti za pojedine korisnike i dodjeljivati administratorske ovlasti za upravljanje mrežnim postavkama.

Promet koji se šalje koji se šalje komunikacijskim kanalom je kriptiran: razmjena ključeva odvija se nakon što su korisnici autenticirani i tunel uspostavljen. Autentikacija korisnika obavlja se razmjenom RSA ključa. Kako bi se prijavio na sustav, korisnik prijavljuje svoju IP adresu (određenu Hamachi programom)

i koristi privatni ključ za prijavu na poslužitelj. Osim toga, svaki paket koji putuje mrežom ima svoju brojevnu oznaku čime se onemogućuje izvođenje napada ponovljenim slanjem istih paketa.

4.5. Ostala VPN rješenja

Iako su u tekstu nabrojana samo neka moguća rješenja za uspostavu VPN veza postoji i niz drugih, kako besplatnih tako i komercijalnih alata:

- Free S/WAN – IPsec VPN primjena VPN-a za operacijske sustave Linux
- Aventail – komercijalan alat namijenjen udaljenim korisnicima i za poslovne partnere trebaju pristup podacima druge tvrtke
- Nokia Mobile VPN – prvenstveno namijenjen za velike tvrtke kada žele omogućiti vezu s manjim podružnicama
- Nortel EAC VPN – za ekstranet mreže

Za više detalja savjetuje se pogledati stranice:

- http://linas.org/linux/vpn.html i
- http://www.vpnlabs.com/vpn-software.html

5. Najčešći sigurnosni propusti

U razdoblju od tri godine NTA Monitor je ispitivao različite VPN sustave i ustanovljeno je kako 90% njih sadrže sigurnosne propuste koje napadači mogu iskoristiti za neovlašteni pristup, pregledavanje/izmjenu podataka te za rušenje VPN poslužitelja.

Kao neke od bitnih propusta navode činjenicu kako se novi korisnici uglavnom dodaju tako da se za korisničko ime koriste osobna imena ili e-mail adrese što napadači mogu lako pogoditi i iskoristiti za napad. U korist tome ide i podatak kako se, uglavnom, kombinacije mogu isprobavati neograničeno bez da se račun zaključa nakon nekog vremena. Osim toga, pojedina VPN rješenja se primjenjuju tako da nakon upisa korisničkih podataka poslužitelj šalje obavijest je li ime ili lozinka neispravno što napadaču također može olakšati posao oko saznavanja tajnih podataka.

U tablici 5. navode se neki od najčešćih propusta/napada u primjeni VPN tehnologije.

Opis	Iskorištavanje propusta
Hakerski napadi upućeni prema klijentu	Najčešće se izvode napadi krađe korisničkih sjednica (napadač preuzima postojeću korisničku sjednicu i postaje autorizirani korisnik na mreži) ili Man-in-the-Middle napad (pri čemu napadač prati pakete te ih može brisati, mijenjati ubacivati nove, itd.)
Autentikacija korisnika	Kod nekih ranije spomenutih protokola, kao što je primjerice PPTP, korisničko ime i lozinka se šalju mrežom bez enkripcije. Potencijalni napadač može tako vrlo jednostavno i brzo saznati sve bitne pristupne podatke te se spojiti na zaštićenu mrežu te tako otkriti osjetljive podatke. Isto tako treba pripaziti da se ti podaci čuvaju u datotekama koje nisu svakom dostupne.
Virusi	Ukoliko je korisnikovo računalo zaraženo virusom vrlo je vjerojatno kako će ga prenijeti i na mrežu na koju se spaja čime se povećava mogućnost curenja povjerljivih podataka kao što su podaci za pristup.
Pristupna prava i ovlasti	Potrebno je strogo kontrolirati tko sve ima pristup na mrežu, ali isto tako od velike je važnosti nadzirati kojim podacima, programima i ostalim resursima mogu pristupiti pojedini korisnici kako ne bi došlo do zlouporabe.
Nekompatibilnost proizvoda	Prilikom nabavke opreme bitno je voditi računa o tome jesu li uređaji različitih proizvođača međusobno kompatibilni za rad. U suprotnom mogući su problemi kod uspostave VPN veze ili ispravne primjene mehanizama koji doprinose zaštiti podataka

Tablica 5. Pregled nekih od najčešćih načina zlouporabe VPN-a

Osnovna ideja svih danas dostupnih VPN rješenja se svodi na zaštitu od pasivnih i aktivnih napada.

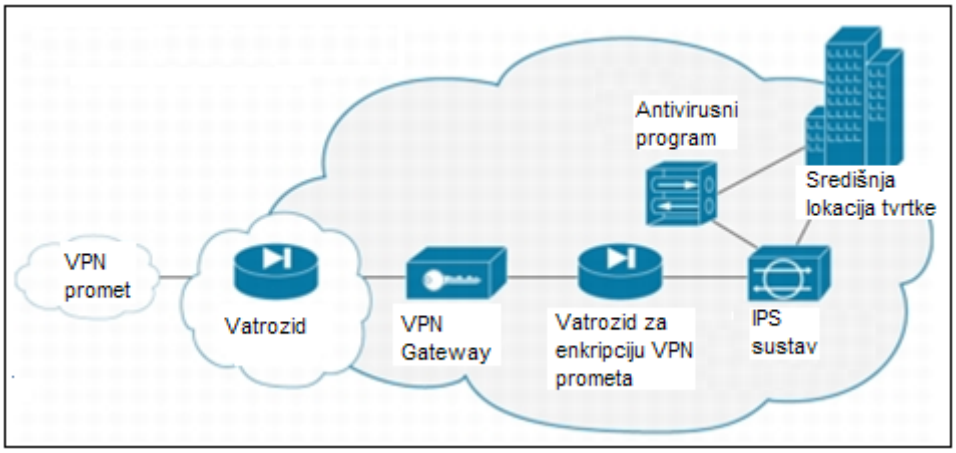
Pasivni napadač je onaj koji osluškuje komunikacijski kanal, ali ne djeluje aktivno na informacije. Kao zaštita, preporuča se korištenje neke od kriptografskih metoda.

Za razliku od toga, aktivni napadač je onaj koji se „ubacuje“ u komunikacijski kanal tako što dodaje, mijenja ili briše podatke koji se šalju. To predstavlja tzv. „Man-in-the-Middle“ napad.

Iz tih se razloga preporuča korištenje dodatnih metoda za povećanje sigurnosti kao što su:

- Korištenje vatrozida
- Korištenje IDS/IPS sustava (eng. Intrusion Detection / Prevention System) kako bi se što učinkovitije kontrolirao promet
- Antivirusni program instaliran na strani klijenta i poslužitelja
- VPN pristupnu točku se preporučuje smjestiti u DMZ zonu kako bi se zaštitila lokalna mreža
- Stroga provjera pristupa za VPN klijente
- Redovna nadogradnja postojećih programa novim zakrpama

U tom bi slučaju mreža trebala izgledati ovako:



Slika 12. Povećanje sigurnosti prilikom korištenja VPN komunikacije

Izvor: Cisco

5.1. Sigurnosni propusti OpenVPN rješenja

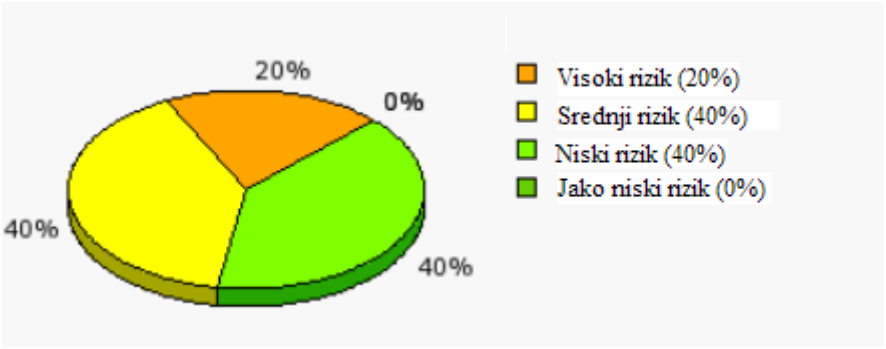
5.1.1. Open VPN 1.x

U razdoblju od 2003. do 2008. godine za OpenVPN inačicu 1.x zabilježen je svega jedan sigurnosni propust. Radi se o DoS (eng. Denial of Service) ranjivosti koju je mogao iskoristiti udaljeni napadač za rušenje ranjivog poslužitelja. Ubrzo nakon otkrivanja propusta proizvođač je objavio odgovarajuću sigurnosnu zakrpu. Važno je napomenuti da tijekom 2008. godine nije zabilježen niti jedan propust u ovoj inačici programa.

5.1.2. OpenVPN 2.x

Od 2003. do 2006. godine za ovu je inačicu otkriveno 5 sigurnosnih propusta. 20% je ocijenjeno visoko rizičnima, 40% se odnosi na ranjivosti srednjeg stupnja rizika te ostatak na niski stupanj rizika (40%).

Propusti su uglavnom omogućavali neovlašten pristup sustavu (43%), izvođenje napada uskraćivanja usluge (43%) i zaobilaženje pojedinih sigurnosnih ograničenja (14%). Za sve je ove sigurnosne nedostatke proizvođač objavio odgovarajuće programske ispravke.



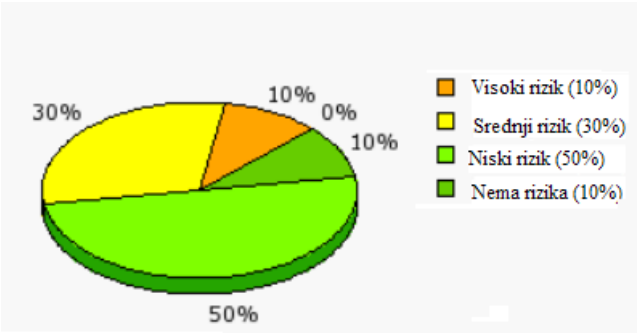
Slika 13. Pregled propusta za OpenVPN prema stupnju rizika
za razdoblje od 1.1.2003. do 31.12.2006.
Izvor: Secunia

U razdoblju 2007. i ove godine za inačicu 2.x nije zabilježena niti jedna sigurnosna ranjivost.

5.2. Cisco Easy VPN

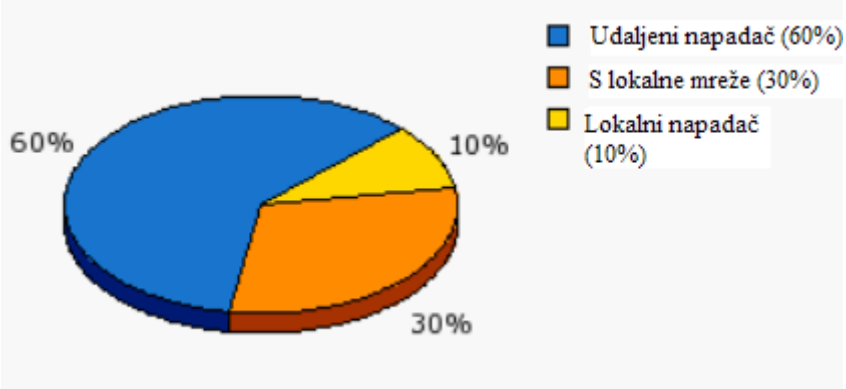
5.2.1. Cisco 3000 Concentrator

Za Cisco Easy VPN programski paket u nastavku navodimo podatke za uređaj Cisco 3000 Concentrator koji ima ulogu na strani poslužitelja. Od 2003. do danas uočeno je 11 sigurnosnih ranjivosti. Za 70% njih proizvođač je objavio ispravke, a dio njih je riješen djelomično ili su napravljene izmjene u samom sustavu kako napadač ne bi mogao iskoristiti propuste. Za jednu ranjivost (10%) nisu objavljene zakrpe. Od toga jedan je propust visokog stupnja rizika, dok su ostali srednjeg (30%) ili niskog stupnja (10%). Jedan od otkrivenih propusta nema negativnog utjecaja na sustav tj. nije ga moguće iskoristiti.



Slika 14. Ranjivosti prema stupnju rizika
za razdoblje od 1.1.2003. do 31.12.2006.
Izvor: Secunia

Na sljedećoj slici vidljivo je na koji je način zlonamjerni korisnik mogao iskoristiti ranjivosti. Dakle, u 60% slučajeva radilo se o udaljenom napadaču, 30% ranjivosti moglo se iskoristiti preko lokalne mreže, a u jednom je slučaju nedostatak iskoristio lokalni napadač.



Slika 15. Cisco 3000 Concentrator – propusti prema vrsti napadača

Izvor: Secunia

Uočeni su propusti omogućavali:

- Neovlašten pristup sustavu . 8%
- DoS napad – 42%
- Otkrivanje osjetljivih podataka – 8%
- Otkrivanje podataka o sustavu – 8%
- XSS napad – 8%
- Zaobilaženje pojedinih sigurnosnih ograničenja – 25%

5.2.2. Cisco VPN Client 4.x

Kod Cisco VPN klijenta inačice 4.x tijekom zadnjih pet godina otkrivena su 4 sigurnosna propusta. Svi su propusti ocijenjeni niskim stupnjem rizika. Za 75% njih je proizvođač objavio programske ispravke kako bi se propust riješio, dok su ostali riješeni djelomično.

Lokalnom su napadaču propusti omogućavali povećanje ovlasti (75%) i otkrivanje osjetljivih podataka o korisniku (25%). Tijekom 2008. godine zabilježena je jedna ranjivost koja je napadaču omogućavala povećanje ovlasti i za nju je objavljena odgovarajuća zakrpa.

5.2.3. Cisco VPN Client 5.x

Za programski paket Cisco VPN Client 5.x instaliran na korisnikovom računalu u zadnjih je pet godina uočeno 3 ranjivosti. Za dio tih nedostataka su objavljene zakrpe (67%), dok je drugi dio ostao još uvijek neriješen (33%). Ovi su propusti imali niski stupanj rizika (67%) ili uopće nisu bili rizični (33%). Ranjivosti je lokalni napadač mogao iskoristiti za povećanje ovlasti na ranjivom sustavu (67%) ili za izvođenje DoS napada (33%).

U 2008 uočena su 2 propusta koja su napadaču omogućila povećanje ovlasti. Od toga je za jednu objavljena zakrpa, a za drugu, koja nije imala nikakvog utjecaja na sigurnost sustava, proizvođač nije izdao zakrpu.

5.3. Microsoft VPN propusti

5.3.1. L2TP/IPsec propusti

Za ovu inačicu VPN rješenja nisu dostupni podaci o propustima za pojedinu godinu. Poznato je samo na koji način napadač najčešće može ugroziti sustav.

Uslijed neodgovarajuće primjene sigurnosnih politika napadaču je omogućen pristup podacima koji se šalju mrežom.

Kao još jedan od učestalih propusta javlja se problem neodgovarajuće primjene filtara što napadaču omogućuje zaobilaženje određenih sigurnosnih ograničenja i time pristup ranjivom sustavu.

5.3.2. PPTP ranjivosti

Iako ne postoje detaljni statistički podaci o propustima poznato je kako je PPTP protokol kod operacijskih sustava Windows ranjiv te kako se najčešće iskorištavaju propusti. Najbitniji među njima su:

1. Izvođenje DoS napada - ranjivost se javlja ukoliko napadač zaguši TCP/IP priključak 1723 ili pregledavanjem i lažiranjem GRE paketa na priključku poslužitelja

2. Pristup osjetljivim podacima - do ranjivosti dolazi otkrivanjem autentikacijskih podataka zbog neodgovarajuće primjene NSHAPv1 i MSCHAPv2 algoritma

5.4. Hamachi – sigurnosni propusti

Za ovaj programski paket dosad je objavljena svega jedna sigurnosna preporuka koja upućuje na ranjivost. Radi se o propustu koji udaljeni napadač može iskoristiti kako bi saznao korisničke zaporke, što mu dalje omogućava spajanje na privatnu mrežu kao da je registrirani korisnik.

Iz svega navedenog i opisanog vidljivo je da većina sigurnosnih incidenata zabilježenih u praksi nisu rezultat sigurnosnih propusta unutar VPN klijenta i/ili poslužitelja već se javljaju zbog pogrešaka u konfiguraciji, nedovoljnom tehničkom znanju krajnjih korisnika ili propusta drugi dijelova računalne mreže.

6. Zaključak

Virtualna privatna mreža pruža zaštitu nad informacijama i podacima koji se prenose Internetom tako što dozvoljava korisnicima uspostavu virtualnog tunela. Na taj se način povećava razina sigurnosti kod preuzimanja zaštićenih podataka tvrtke ili organizacije. Isto tako, VPN zahtijeva dobro razumijevanje problema sigurnosti javih mreža i poduzimanje mjera opreza kod postavljanja.

S obzirom da daljnji uspjeh VPN-a u budućnosti uvelike ovisi o razvoju tehnologija, svima se preporuča praćenje novih trendova i novih primjena koje mogu dodatno unaprijediti sigurnost kod razmjene onih podataka koji trebaju biti dostupni samo pojedinim korisnicima.

7. Reference

[1] Cisco,http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/prod_white_paper0900aecd804fb79a_ns461_Networking_Solutions_White_Paper.html, studeni 2007.

[2] Tech Republic, http://articles.techrepublic.com.com/5100-10878_11-1059747.html, kolovoz 2002.

[3] Ana Kukec, http://os2.zemris.fer.hr/ns/2006_kukec/, siječanj 2006.

[4] Real Time Enterprises, http://www.real-time.com/security/pptp.html, ožujak 2008.

[5] Real Time Enterprises, http://support.real-time.com/windows/vpn/windows_xp_vpn.html, lipanj 2007.

[6] Technet, http://technet.microsoft.com/en-us/library/bb742553.aspx, siječanj 2008.

[7] Wikipedia, http://en.wikipedia.org/wiki/Cisco_Systems#Cisco_Systems_VPN_Client, kolovoz 2008.

[8] Matija Zeman, http://os2.zemris.fer.hr/ns/firewall/2006_zeman/index.html, prosinac 2006.

[9] About.com, http://compnetworking.about.com/od/vpn/a/what_is_a_vpn.htm, veljača 2008.

[10] NTA Monitor, http://www.nta-monitor.com/posts/2005/01/vpn-flaws.html, siječanj 2005.

[11] KSFB, http://www.ksfb.rs/forum/index.php?topic=1448.0, ožujak 2008.

[12] Cisco, http://www.cisco.com/en/US/docs/ios/12_2t/12_2t8/feature/guide/ftunity.html, lipanj 2007.

[13] SC, http://www.scmagazine.com/asia/news/article/419761/making-right-connection-vpn-ssl-ipsec-both , prosinac 2005.

[14] Hamachi, https://secure.logmein.com/products/hamachi/advantages.asp, siječanj 2008.

[15] Hamachi, https://secure.logmein.com/products/hamachi/security.asp, siječanj 2008.

[16] Hamachi, https://secure.logmein.com/products/hamachi/howitworks.asp, siječanj 2008.

[17] Frane Urem, http://www.vus.hr/uploads/file/zbornik/rad_frane_urem.pdf, lipanj 2006.

[18] Best Computer EBooks, www.bojonegoro.go.id/book/tunneling_basic.php, prosinac 2007.

[19] Secunia, http://secunia.com/advisories/product/5568/, veljača 2008.

[20] Secunia, http://secunia.com/advisories/product/3952/?task=statistics, ožujak 2008.

[21] Secunia, http://secunia.com/advisories/product/90/?task=statistics_2003, ožujak 2008.

[22] Secunia, http://secunia.com/advisories/product/14325/, siječanj 2008.